National Practitioner Data Bank-Healthcare Integrity and Protection Data Bank (NPDB-HIPDB)

Integrated Querying and Reporting Service (IQRS)
User Review Panel (URP)

NPDB-HIPDB Security

Sandy Rosenblatt

November 9, 2005

NPDB-HIPDB Security

- **Planning Security Enhancements.**

- **Recent Security Enhancements.**

- **Future Security Enhancements.**

- **Important Security Reminders.**

Planning Security Enhancements

- **NPDB-HIPDB required to meet federal regulations and guidelines.**

- **NPDB-HIPDB System Security Plan documents security controls.**

- **Security Review required annually.**
  - Assessments conducted by independent analysts.
  - Verifies security controls meet required regulations.
  - Results of assessments dictate future security enhancements.

- **Certification and Accreditation required every 3 years.**
  - Grants authorization to operate and maintain the system.
  - Based on successful completion of Security Review.
  - Current Certification and Accreditation granted June 2004.

Planning Security Enhancements

- Self Assessment.

- Privacy Impact Assessment.

- Risk Assessment.

- Security Test and Evaluation.

- Technical Vulnerability Assessment.

Planning Security Enhancements

- Results of assessments are documented and reviewed.

- Security enhancements are identified, prioritized, and assigned a completion date.

- Plan of Actions and Milestones used to track status of security enhancements.

- Plan of Actions and Milestones sent to HRSA and HHS Quarterly.

Recent Security Enhancements

- Confidential Passwords.

- Password Rules.

- Password Expiration.

- Customer Service Center Functions.

- IQRS Security Notice.

- Internal System Upgrades.

Recent Security Enhancements

Confidential Passwords

- Passwords can only be viewed by an individual user.

- NPDB-HIPDB Customer Service Center has no access to user passwords.

- Entity's Administrator cannot view passwords.

- Agent cannot view Entity's passwords.

- New or reset password is randomly generated, must be reset immediately after logging on to the IQRS.

Recent Security Enhancements

Password Rules

- Must be 8-14 characters, at least 1 alphabetic and 1 numeric character.

- Must be different from the previous 4 passwords.

- Must not be a word found in the dictionary.

- Must not be a common Data Bank phrase.

- Must not be your User ID.

- Must not be a simplistic sequence (abcd1234).

Recent Security Enhancements

Password Expiration

	Expiration	Expiration Notice	Grace Login	One Time Use
General Password	90 calendar days	5 calendar days prior to expiration	30 calendar days after expiration	N/A
New Entity Password	30 calendar days	N/A	No	Yes
Reset Password	3 calendar days	N/A	No	Yes

Recent Security Enhancements

Customer Service Center Functions

- Access to a read-only version of the IQRS.

- Provides capability to walk through any process.

- Can not update or modify any data.

- Can not submit queries or reports.

Recent Security Enhancements

IQRS Security Notice

- Mechanism to communicate security changes and best practices to users.

- Available from the Entity and Agent Registration Confirmation Screens.

- Recent Topics Include:
    - Data Bank Confidentiality.
    - Entity Administrator Responsibilities.
    - Password Expiration.
    - Creating Secure Passwords.
    - Other Security Pointers.

Recent Security Enhancements

Internal System Upgrades

- Production Firewall upgrades.

- Passwords are encrypted.

- Automated patch management for NPDB-HIPDB desktops.

Future Security Enhancements

- IQRS Rules of Behavior.

- Registration Rules of Behavior.

- Internal System Upgrades.

Future Security Enhancements

IQRS Rules of Behavior

- All Data Banks' users must agree to comply with the Rules of Behavior.

- Rules of Behavior can be viewed from the Informational Web Site.

- New IQRS Users must acknowledge the Rules of Behavior after first login.

- Existing IQRS Users must acknowledge the Rules of Behavior every 12 months.

IQRS Rules of Behavior

IQRS Rules of Behavior

Login - Microsoft Internet Explorer

LOGIN

**National Practitioner Data Bank
Healthcare Integrity and Protection Data Bank**

Welcome to the Integrated Querying and Reporting Service (IQRS)

Only specific entities authorized by law may request the disclosure of information from (i.e., query) or submit reports to the National Practitioner Data Bank (NPDB) or the Healthcare Integrity and Protection Data Bank (HIPDB).

Authorized entities must be registered with the appropriate Data Bank(s) and have received a confidential Data Bank Identification Number (DBID) and password prior to using this querying and reporting service. All individuals that have access to obtain information from and report information to the NPDB-HIPDB system must acknowledge and comply with the Rules of Behavior.

Any unauthorized individual or organization that attempts to query or file reports with the Data Bank(s) is subject to fine and imprisonment under Federal statute.

If you are not authorized by law and registered to query or report to either the NPDB or the HIPDB, **DO NOT ATTEMPT TO ACCESS THIS SERVICE.**

Data Bank Identification Number

User ID

User Password

Login

To ensure that all features of this site work properly, use one of the following supported browser versions: Netscape 7.02, 7.1, 7.2, or Internet Explorer 6.0, 6.0 SP1, or 6.0 SP2.

Getting Help

Help ?
Click the Help icon to obtain information related to a screen.

Go to the NPDB-HIPDB home page.

Home

IQRS Rules of Behavior

RULES OF BEHAVIOR

National Practitioner Data Bank
Healthcare Integrity and Protection Data Bank

All individuals that have access to obtain information from and report information to the NPDB-HIPDB system must comply with the following conditions:

- **Ownership**

This system is the property of the US Department of Health and Human Services, Health Resources and Services Administration and is for authorized users only. The system is for official NPDB-HIPDB business only. Unauthorized access or use of this system may subject violators to criminal, civil and/or administrative penalties.

- **Responsibilities**

Individual users are provided with a unique user id and initial password to access this system. The first time you login to the system, you will be forced to establish your own password to continue to use the system. You are responsible for maintaining the integrity of and are held accountable for everything done using your user id and password. No other person, including those at the NPDB-HIPDB Customer Service Center has access to your password. Passwords shall not be shared with others. If password security is suspected to be compromised you agree to change the password immediately, and notify the NPDB-HIPDB Customer Service Center.

Information and activities associated with the NPDB-HIPDB system shall not be false, inaccurate or misleading; violate any law, statute, ordinance or regulation; and contain any viruses or any malicious code that may damage, detrimentally interfere with, surreptitiously intercept, or expropriate any system, data, or personal information. "Information" is defined as any information you provide to the NPDB-HIPDB System in the course of using this system. "Activities" is defined as any process of interacting with the NPDB-HIPDB system.

This page is displayed immediately upon login.

IQRS Rules of Behavior

Rules of Behavior - Microsoft Internet Explorer

- **Confidentiality**

The system contains personal information protected under the provisions of *the Privacy Act of 1974*, 5 USC Section 552a. Violations of the provisions of the *Privacy Act* may subject the offender to criminal penalties.

Information reported to the NPDB and the HIPDB is confidential and shall not be disclosed except as specified in the NPDB and HIPDB regulations. The HHS OIG has the authority to impose civil money penalties on those who violate the confidentiality provisions of NPDB and/or HIPDB information. Persons or entities that receive information either directly or indirectly are subject to the confidentiality provisions specified in the NPDB regulations at 45 CFR Part 60 and the imposition of a civil money penalty of up to $11,000 for each offense if they violate those provisions. When an authorized agent is designated to handle NPDB-HIPDB queries, both the entity and the agent are required to maintain confidentiality in accordance with the federal statutory requirements.

- **Intrusion Detection**

This site is maintained for the U.S. Government. It is protected by various provisions of Title 18, US Code. Violations of Title 18 are subject to criminal prosecution in federal court.

Individuals using this system are subject to monitoring of those activities. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence obtained by such monitoring to law enforcement officials. Moreover, for system security purposes and to ensure that the system is used for legitimate purposes by authorized, registered users, we collect information concerning the use of this system e.g. data you view and alter. We employ software programs to monitor traffic, and to identify unauthorized attempts to view and/or change information, or otherwise cause damage to the system. Information from these sources may be used to help identify an individual(s) in the event of authorized law enforcement investigation, and pursuant to any required legal process.

IQRS Rules of Behavior

This site is maintained for the U.S. Government. It is protected by various provisions of Title 18, US Code. Violations of Title 18 are subject to criminal prosecution in federal court.

Individuals using this system are subject to monitoring of those activities. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence obtained by such monitoring to law enforcement officials. Moreover, for system security purposes and to ensure that the system is used for legitimate purposes by authorized, registered users, we collect information concerning the use of this system e.g. data you view and alter. We employ software programs to monitor traffic, and to identify unauthorized attempts to view and/or change information, or otherwise cause damage to the system. Information from these sources may be used to help identify an individual(s) in the event of authorized law enforcement investigation, and pursuant to any required legal process.

- **Violation of Rules of Behavior**

In the event it is suspected that you have not complied with these rules of behavior your account will be frozen, resulting in denial of all access to the system; and criminal, civil and/or administrative action may be taken.

☐ I acknowledge and understand my responsibilities and agree to comply with the Rules of Behavior for the NPDB-HIPDB system.

Continue

End Session & Return to Login

IQRS Rules of Behavior

Rules of Behavior - Microsoft Internet Explorer

This site is maintained for the U.S. Government. It is protected by various provisions of Title 18, US Code. Violations of Title 18 are subject to criminal prosecution in federal court.

Individuals using this system are subject to monitoring of those activities. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence obtained by such monitoring to law enforcement officials. Moreover, for system security purposes and to ensure that the system is used for legitimate purposes by authorized, registered users, we collect information concerning the use of this system e.g. data you view and alter. We employ software programs to monitor traffic, and to identify unauthorized attempts to view and/or change information, or otherwise cause damage to the system. Information from these s[...] f authorized law enforcement investigatio[...]

Microsoft Internet Explorer

You must click the checkbox to accept the rules of behavior before continuing.

OK

- **Violation of Rules o**

In the event it is suspect[...] [...]count will be frozen, resulting in denial of all access to the system; and criminal, civil and/or administrative action may be taken.

☐ I acknowledge and understand my responsibilities and agree to comply with the Rules of Behavior for the NPDB-HIPDB system.

Continue

End Session & Return to Login

IQRS Rules of Behavior

Rules of Behavior - Microsoft Internet Explorer

This site is maintained for the U.S. Government. It is protected by various provisions of Title 18, US Code. Violations of Title 18 are subject to criminal prosecution in federal court.

Individuals using this system are subject to monitoring of those activities. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence obtained by such monitoring to law enforcement officials. Moreover, for system security purposes and to ensure that the system is used for legitimate purposes by authorized, registered users, we collect information concerning the use of this system e.g. data you view and alter. We employ software programs to monitor traffic, and to identify unauthorized attempts to view and/or change information, or otherwise cause damage to the system. Information from these sources may be used to help identify an individual(s) in the event of authorized law enforcement investigation, and pursuant to any required legal process.

- **Violation of Rules of Behavior**

In the event it is suspected that you have not complied with these rules of behavior your account will be frozen, resulting in denial of all access to the system; and criminal, civil and/or administrative action may be taken.

☑ I acknowledge and understand my responsibilities and agree to comply with the Rules of Behavior for the NPDB-HIPDB system.

Continue

End Session & Return to Login

IQRS Rules of Behavior

Future Security Enhancements

Registration Rules of Behavior

- All Data Banks' users must agree to comply with the Rules of Behavior.

- Entity Registrants must acknowledge the Rules of Behavior prior to filling out the registration form.

- Agent Registrants must acknowledge the Rules of Behavior prior to filling out the registration form.

Registration Rules of Behavior

Registration Rules of Behavior

Registration Rules of Behavior

Rules of Behavior - Microsoft Internet Explorer

RULES OF BEHAVIOR

**National Practitioner Data Bank
Healthcare Integrity and Protection Data Bank**

All individuals that have access to obtain information from and report information to the NPDB-HIPDB system must comply with the following conditions:

- **Ownership**

This system is the property of the US Department of Health and Human Services, Health Resources and Services Administration and is for authorized users only. The system is for official NPDB-HIPDB business only. Unauthorized access or use of this system may subject violators to criminal, civil and/or administrative penalties.

- **Responsibilities**

Information and activities associated with the NPDB-HIPDB system shall not be false, inaccurate or misleading; violate any law, statute, ordinance or regulation; and contain any viruses or any malicious code that may damage, detrimentally interfere with, surreptitiously intercept, or expropriate any system, data, or personal information. "Information" is defined as any information you provide to the NPDB-HIPDB System in the course of using this system. "Activities" is defined as any process of interacting with the NPDB-HIPDB system.

- **Confidentiality**

The system contains personal information protected under the provisions of *the Privacy Act of 1974*, 5 USC Section 552a. Violations of the provisions of the *Privacy Act* may subject the offender to criminal penalties.

Information reported to the NPDB and the HIPDB is confidential and shall not be disclosed except as

Registration Rules of Behavior

Rules of Behavior - Microsoft Internet Explorer

This site is maintained for the U.S. Government. It is protected by various provisions of Title 18, US Code. Violations of Title 18 are subject to criminal prosecution in federal court.

Individuals using this system are subject to monitoring of those activities. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence obtained by such monitoring to law enforcement officials. Moreover, for system security purposes and to ensure that the system is used for legitimate purposes by authorized, registered users, we collect information concerning the use of this system e.g. data you view and alter. We employ software programs to monitor traffic, and to identify unauthorized attempts to view and/or change information, or otherwise cause damage to the system. Information from these sources may be used to help identify an individual(s) in the event of authorized law enforcement investigation, and pursuant to any required legal process.

- **Violation of Rules of Behavior**

In the event it is suspected that you have not complied with these rules of behavior your account will be frozen, resulting in denial of all access to the system; and criminal, civil and/or administrative action may be taken.

☑ I acknowledge and understand my responsibilities and agree to comply with the Rules of Behavior for the NPDB-HIPDB system.

Continue

Return to NPDB-HIPDB Home Page

Registration Rules of Behavior

Future Security Enhancements

Internal System Upgrades

■ Intrusion Detection Server upgrade.

■ Database upgrade.

■ Credit Card processing interface upgrade.

■ All internal communications encrypted.

Important Security Reminders

- **Password tips:**
  - Use upper and lower case letters, and special characters.
  - Do not use personal information—your name, names of family members, entity name, birth date, etc.
  - Do not share your password.
  - Do not write down your password, remember it.

- **Make your password easy to remember:**
  - Make up nonsense words that are pronounceable, such as "BingZing3!" or "ZorP@GorP8".
  - Combine two short words with special characters, such as "4Truck+in" or "mY2birdS!".
  - Pick a phrase and use the first letter of each word. For example, "Will It Rain Today" could produce "W+i+r+t?04".

Important Security Reminders

- Log out of the IQRS at the end of the session.

- Verify the date and time when your account was last accessed.

- Do not share Data Bank reports.

- Securely store or shred Data Bank Reports.

NPDB-HIPDB Security

Questions / Comments